

Обеспечение квантовой устойчивости ключевых цифровых экосистем и платформ Экономики данных является одной из серьезных научно-технических проблем современности, анализ состояния которой позволил выделить три возможных направления ее разрешения.

Во-первых, создание и переход на постквантовые криптопримитивы и электронной подписи на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых в настоящее время неизвестны эффективные алгоритмы решения на классических и квантовых вычислителях. *Во-вторых*, создание и переход на единичные квантово-устойчивые компоненты и связи упомянутых систем с математически доказуемой стойкостью. *В-третьих*, создание и программно-техническая реализация принципиально новых квантово-механических моделей ключевых цифровых экосистем и платформ Экономики данных Российской Федерации на физических принципах и законах квантовой механики.

В пособии обсуждаются все три перечисленных направления и представлены возможные решения рассматриваемой научно-технической проблемы.

Введение

Определения, обозначения и сокращения

Глава 1. Разработка Концепции обеспечения квантовой устойчивости цифровых платформ «Экономики данных» РФ

- 1.1. Роль и место сквозной информационной технологии блокчейн
- 1.2. Актуальность проблемы обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ
- 1.3. Потенциальные потребители создаваемых научно-технических результатов
- 1.4. Сопроблемы квантовой устойчивости блокчейн-экосистем
- 1.5. Основные этапы разрешения научной проблемы
- 1.6. Основные направления исследований

Глава 2. Моделирование угроз безопасности информации национальных блокчейн-экосистем и платформ в условиях появления новой квантовой угрозы

- 2.1. Модель угроз безопасности информации для типовой национальной блокчейн-платформы
- 2.2. Микромодель угроз безопасности информации для типовой блокчейн-платформы на основе математического аппарата сетей Петри
- 2.3. Макромодель угроз безопасности информации национальных блокчейн-экосистем и платформ на основе динамических взаимосвязей Р. Калмана и теории катастроф Р. Тома и В. Арнольда

Список литературы к главам 1 и 2

Глава 3. Решение задач анализа квантовой устойчивости национальных блокчейн-экосистем и платформ

- 3.1. Метод анализа квантовой устойчивости национальных блокчейн-экосистем и платформ
- 3.2. О применении в криптологии квантового преобразования Фурье
- 3.3. Решение оптимизационных задач обеспечения квантовой устойчивости национальных блокчейн-платформ методом квантового отжига

Список литературы к главе 3

Глава 4. Решение задач синтеза квантово-устойчивых национальных блокчейн-экосистем и платформ

- 4.1. Алгебраический алгоритм ЭЦП с двумя скрытыми группами
- 4.2. Типовые уравнения верификации в алгебраических схемах ЭЦП с двумя скрытыми группами
- 4.3. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами

Список литературы к главе 4

Заключение

- Приложение А.** Характеристика объекта исследования: национальных блокчейн-экосистем платформ
- Приложение Б.** Концептуальная модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ
- Приложение В.** Функциональная спецификация к инструментальным средствам обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ Цифровой экономики РФ
- Приложение Г.** Состав программных компонент (модулей) перспективного программного комплекса обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ в условиях появления новой квантовой угрозы безопасности информации
- Приложение Д.** Свидетельства о государственной регистрации программ для ЭВМ